UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,371	10/07/2003	Anthony C. Fascenda	62922.3	4292

21967 7590 11/24/2004

HUNTON & WILLIAMS LLP
INTELLECTUAL PROPERTY DEPARTMENT
1900 K STREET, N.W.
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/679,371	FASCENDA, ANTHONY C.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11, and 13-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 13-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11, 13-28 have been examined.

2. Claim 12 is orally withdrawn by election of restriction over the phone on11/15/2004.

Election/Restrictions

3. Restriction to one of the following invention is required under 35 U.S.C. 121:

   I. Claim 1 –11, 13-28 drawn to authentication protocol using challenge-response scheme, classified under 713/155.

   II. Claim 12 drawn to encryption key generation, classified under 380/44.

4. Inventions I and II are related as subcombination disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. The following case instants:

5. Invention I has separate utility such as challenge and response for authentication and Invention II generates key to encrypt data.

6. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

7. Claim 12 is orally withdrawn by election of restriction over the phone on11/15/2004.

8. Claim 12 is withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made with traverse.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-11, 13, and 19-28 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Pitchenik et al. U.S. Pat. No. 6397328 (hereinafter Pitchenik).

11. As per claim 1, Pitchenik discloses a method of authenticating computing devices on a communications network comprising the steps of : receiving a first challenge from a computing device, wherein said first challenge comprises an encrypted first random number and a unique identifier associated with said computing device (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67); obtaining a first secret cryptographic key associated with said unique identifier (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67); generating a second random number (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 –

67); decrypting said first random number with said first secret cryptographic key (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67); encrypting said second random number with said first secret cryptographic key (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67); and transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said second random number (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67).

12. As per claim 19, Pitchenik discloses a method of authenticating computing devices on a communications network comprising the steps of: receiving a first challenge from a computing device, wherein said first challenge comprises a first random number and a unique identifier associated with said first secret cryptographic key (Pitchenik: column 2 line 34 – column 3 line 3); and transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted first random number and said second random number (Pitchenik: column 2 line 34 – column 3 line 3).

13. As per claim 2 and 20, Pitchenik discloses the method of claims 1 and 19 respectively. Pitchenik further discloses wherein said unique identifier is a serial number of a physical token installed at said computing device (Pitchenik: column 3 line 60 – column 4 line 10: the identification number and associated key within the device).

14. As per claim 3 and 21, Pitchenik discloses the method of claims 2 and 20 respectively. Pitchenik further discloses wherein said step of obtaining a first secret cryptographic key

comprises the step of retrieving a pre-stored record associated with said serial number, wherein said record comprises said first secret cryptographic key (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10: the keys are stored in the device and the host PC respectively).

15. As per claim 4 and 22, Pitchenik discloses the method of claims 3 and 21 respectively. Pitchenik further discloses wherein said step of obtaining a first secret cryptographic key comprises the step of receiving a key database file comprising a number of records, wherein each record is associated with a unique physical key token and comprises a unique secret cryptographic key and a unique serial number (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10: the keys are stored in the device and the host PC respectively).

16. As per claim 5 and 23, Pitchenik discloses the method of claims 4 and 22 respectively. Pitchenik further discloses wherein said unique secret cryptographic key is created from a random number generated at initialization of said token (Pitchenik: column 3 line 60 – column 4 line 24).

17. As per claim 6 and 24, Pitchenik discloses the method of claims 1 and 19 respectively. Pitchenik further discloses the method comprising the steps of: decrypting said first challenge with a network receive cryptographic key; and encrypting said second challenge with a network

send cryptographic key (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10: the key pair).

18. As per claim 7, Pitchenik discloses the method of claim 3. Pitchenik further discloses wherein said step of decrypting said encrypted first random number results in a first value, and further comprising the step of disallowing said computing device to communicate with other computing devices on said network if said first value is a null value (Pitchenik: column 4 line 33 – column 5 line 4: the authentication technique can be applied to both parties).

19. As per claim 8, Pitchenik discloses the method of claim 7. Pitchenik further discloses wherein allowing said computing device to communicate with other computing devices on said network if said first value is not a null value (Pitchenik: column 4 line 33 – column 5 line 4: the authentication technique can be applied to both parties).

20. As per claim 9, Pitchenik discloses the method of claim 7. Pitchenik further discloses the method comprising the step of decrypting said second challenge with a network receive cryptographic key (Pitchenik: Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10: the key pair).

21. As per claim 10, Pitchenik discloses the method of claim 8. Pitchenik further discloses the method comprising the step of decrypting said encrypted second random number with a

second secret cryptographic key (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10).

22. As per claim 11, Pitchenik discloses the method of claim 10. Pitchenik further discloses wherein said second secret cryptographic key is stored within said physical token (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10).

23. As per claim 13, Pitchenik discloses a communications system comprising: a number of computing devices, and at least one authentication device, wherein each client device or authentication device includes a unique tamper-resistant physical token comprising a random number generator, a unique secret cryptographic key, and a unique serial number (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10).

24. As per claim 25, Pitchenik discloses the method of claim 21. Pitchenik further discloses the method comprising the steps of: receiving a third challenge from said computing device, wherein said third challenge comprises said second random number encrypted with a second secret cryptographic key (Pitchenik: column 2 line 34 – column 3 line 29); decrypting said encrypted second random number with said first secret cryptographic key (Pitchenik: column 2 line 34 – column 3 line 29); and comparing said decrypted second random number to said second random number to determine if a match exists (Pitchenik: column 2 line 34 – column 3 line 29).

25. As per claim 26, Pitchenik discloses the method of claim 25. Pitchenik further discloses wherein if a match exists between said decrypted second random number and said second random number, allowing said computing device to communicate with other computing device on said network, otherwise if a match does not exist, disallowing said computing device to communicate with other computing devices on said network (Pitchenik: column 2 line 34 – column 3 line 29).

26. As per claim 27, Pitchenik discloses the method of claim 25. Pitchenik further discloses the method comprising the step of decrypting said third challenge with a network receive cryptographic key (Pitchenik: column 2 line 34 – column 3 line 29).

27. As per claim 28, Pitchenik discloses the method of claim 25. Pitchenik further discloses wherein said second secret cryptographic key is stored within said physical token (Pitchenik: column 2 line 34 – column 3 line 29 and column 3 line 60 – column 4 line 10).

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

29. Claims 14-16, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik in view of Kimura U.S. Pub. No. 20010048744 (hereinafter Kimura).

30. As per claim 14, Pitchenik discloses the system of claim 13. Pitchenik does not explicitly disclose wherein each client device or authentication device further includes a wireless communications transceiver to communicate on a wireless network. However, it would have been obvious to one having ordinary skill in the art to apply the authentication method to any communication environment including wireless network. Alternatively, Kimura discloses access point authentication method and applying challenge response and random numbers to authenticate mobile terminals within wireless LAN that complies with IEEE 802.11 (Kimura: [0038]-[0040]). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to apply the authentication technique to any communication system. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Kimura within the system of Pitchenik because it prevents unauthorized access from mobile stations of malicious intruders in a radio-based wireless LAN network.

31. As per claim 15, Pitchenik as modified discloses the system of claim 14. Pitchenik as modified further discloses wherein said wireless network is Wi-Fi network (Kimura: figure 5 and [0004], [0035]-[0040]).

32. As per claim 16, Pitchenik as modified discloses the system of claim 15. Pitchenik as modified further discloses wherein said authentication device is an access point (Kimura: [0039]-[0040] and figure 2).

33. As per claim 18, Pitchenik as modified discloses the system of claim 16. Pitchenik as modified further discloses wherein said access point includes a database file comprising said serial numbers and secret cryptographic keys associated with said tokens (Pitchenik: column 3 line 60 – column 4 line 10; Kimura: [0004], [0035]-[0040]).

34. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik in view of Kimura and further in view of Shteyn U.S. Pub. No. 20040203590 (hereinafter Shteyn).

35. As per claim 17, Pitchenik as modified discloses the system of claim 13. Pitchenik as modified does not explicitly disclose wherein each tamper-resistant physical token is installed via a USB interface. However, Shteyn discloses using a dongle installed via a USB to secure communications in a wireless network (Shteyn: [0027]). It would have been obvious to one having ordinary skill in the art to store identifications information and cryptographic key into the hardware key while authentication takes place between a mobile terminal and an access point. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shteyn within the combination of Pitchenik-Kimura because dongle is well known in the art for providing security parameters within network.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Merriam U.S. Pat. No. 6643781 discloses a processor generating a random number and send the encrypted random number as challenge and upon receiving the encrypted random number, decrypt it and re-encrypt it and send it back to the processor (column 5 line 62 – column 6 line 21).

Richards U.S. Pub. No. 20010054147 discloses comparing decrypted random number when authenticating a user.

Saito U.S. Pub. No. 20030070067 discloses using device ID to retrieve private key from database ([0085]-[0087]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100